

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of

Docket No.: P27325

J. L. CALVIGNAC et al.

Confirmation No.: 6208

Serial No.: 09/771,472

Group Art Unit: No. 2134

Filed: January 26, 2001

Examiner: E. C. Tran

For: **SINGLE-CYCLE HARDWARE IMPLEMENTATION OF CRYPTO FUNCTION
FOR HIGH THROUGHPUT CRYPTO-PROCESSING**

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Window, Mail Stop Appeal Brief-Patents
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Sir:

This appeal is from the Examiner's final rejection of claims 1-20 as set forth in the Final Office Action of June 13, 2006. A Notice of Appeal and a Request For Pre-Appeal Brief Review, in response to the June 13, 2006 Final Office Action, was filed on October 13, 2006.

Payment in the amount of \$ 500.00 is being concurrently submitted as payment of the requisite fee under 37 C.F.R. 41.20(b)(2). No additional fee is believed to be required for filing the instant Appeal Brief. However, if for any reason a necessary fee is required for consideration of the instant paper, authorization is hereby given to charge the fee for the Appeal Brief and any necessary extension of time fees to Deposit Account No. 50-0563.

TABLE OF CONTENTS

I	REAL PARTY IN INTEREST	Page 3.
II	RELATED APPEALS AND INTERFERENCES	Page 3.
III	STATUS OF CLAIMS	Page 3.
IV	STATUS OF THE AMENDMENTS.....	Page 3.
V	SUMMARY OF THE CLAIMED SUBJECT MATTER.....	Pages 3-5.
VI	GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	Page 5.
VII	ARGUMENTS RE. § 102 REJECTION	Pages 5-32.
VIII	CONCLUSION	Page 32.
	CLAIMS APPENDIX	Pages 33-35.
	EVIDENCE APPENDIX	Page 36.
	RELATED PROCEEDINGS APPENDIX	Page 37.

(I) REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation by an assignment recorded in the U.S. Patent and Trademark Office on January 26, 2001, at Reel 011498 and Frame 0541.

(II) RELATED APPEALS AND INTERFERENCES

No related appeals and/or interferences are pending.

(III) STATUS OF THE CLAIMS

Claims 1-20 are pending. Claims 1-20 stand finally rejected. Thus, finally rejected claims 1-20 are at issue in the instant appeal and form the subject matter of the instant Appeal Brief. The claims in issue are attached in the "Claims Appendix".

(IV) STATUS OF THE AMENDMENTS

A Response under 37 C.F.R. § 1.116 was filed July 26, 2006, requesting reconsideration of the finally rejected claims. The Examiner responded with an Advisory Action mailed August 16, 2006, indicating that the Response was considered, but did not place the application in condition for allowance. Appellant submits that no amendments after final have been filed; however, all amendments to the claims have been entered.

(V) SUMMARY OF THE CLAIMED SUBJECT MATTER

A. The Claimed Subject Matter

INDEPENDENT CLAIM 1

With reference to page 4, line 19 to page 8, line 22 of the instant application and to Figs 1-2, and by way of non-limiting example, the invention provides for a hardware implementation

of a crypto-function comprising a first register (102 and/or 103) storing data to be encrypted or decrypted (see Fig. 1 and page 4, lines 24-25), a second register (204) for receiving data which has been encrypted or decrypted (see Fig. 2 and page 7, line 23 to page 8, line 3), and combinational logic (105, 107, 111, 113, 114, 116) performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle (see page 3, lines 15-20).

INDEPENDENT CLAIM 16

With reference to page 4, line 19 to page 8, line 22 of the instant application and to Figs 1-2, and by way of non-limiting example, the invention provides for a hardware implementation of a crypto-function comprising a first register (102 and/or 103) storing data to be encrypted or decrypted (see Fig. 1 and page 4, lines 24-25), a second register (204) for receiving data which has been encrypted or decrypted (see Fig. 2 and page 7, line 23 to page 8, line 3), and combinational logic (105, 107, 111, 113, 114, 116) performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle (see page 3, lines 15-20). The crypto-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read (see page 2, lines 14-23).

INDEPENDENT CLAIM 19

With reference to page 4, line 19 to page 8, line 22 of the instant application and to Figs 1-2, and by way of non-limiting example, the invention provides for a hardware implementation of a crypto-function comprising a first register (102 and/or 103) storing data to be encrypted or

decrypted (see Fig. 1 and page 4, lines 24-25), a second register (204) for receiving data which has been encrypted or decrypted (see Fig. 2 and page 7, line 23 to page 8, line 3), and combinational logic (105, 107, 111, 113, 114, 116) performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle (see page 3, lines 15-20). The single hardware cycle comprises several clock cycles (see page 2, lines 14-23).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-20 are improperly rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,870,929 issued to GREENE.

Appellant acknowledges that the Notice of Panel Decision from Pre-Appeal Brief Review dated November 20, 2006 specifically states that the Section 112, 2nd paragraph, rejection asserted in the Final Office Action has been withdrawn and is therefore not in issue for this Appeal.

(VII) ARGUMENT RE. 102(e) REJECTION

REJECTION OF INDEPENDENT CLAIM 1 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 1 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited first and second registers and the recited combinational logic. Appellant respectfully disagrees and traverses this rejection.

Appellant acknowledges that GREENE discloses an arrangement which utilizes an

encryption circuit 102, an input buffer 104 and an output buffer 108 (see col. 5, lines 4-12).

Appellant also acknowledges that GREENE discloses that the encryption circuit 102 utilizes “data encryption algorithms such as DES and Triple DES, or any of various secure hash algorithms” (see col. 6, lines 58-62). However, GREENE simply does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle.

The Examiner explains that the disclosed encryption circuit 102 of GREENE is same as the recited combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle. Appellant respectfully disagree. An encryption circuit is not the *per se* same as combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle. As explained on page 2, lines 2-9 of the instant application, conventional processing of crypto-functions require many clock and hardware cycles. As such processing typically occurs in an encryption circuit, the Examiner’s apparent or implicit belief that all encryption circuits perform computation iterations of the crypto-function in a single hardware cycle lacks any support in the prior art.

Furthermore, while the Examiner has specifically pointed to col. 4, line 58 to col. 5, line 13 of GREENE (see page 2 of the Final Office Action) as disclosing the recited computation, the Examiner has failed to fully appreciate the fact that the noted language is entirely silent with regard to the terms “computational logic” and “crypto-function” and merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can

provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input buffer/working store 104, an output buffer 108, and a scheduler 106. An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L , where $L=nT$. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

There is simply no such disclosure in the above-noted language of GREENE and the Examiner has not demonstrated otherwise.

Appellant submits that it is apparent from a fair reading the instant Final Office Action that the Examiner does not fully understand the requirements for a proper anticipation rejection. Appellant directs the Board's attention to MPEP 2131 which specifically states:

TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art." *Brown v. 3M*, 265 F.3d 1349, 1351, 60 USPQ2d 1375, 1376 (Fed. Cir. 2001) (claim to a system for setting a computer clock to an offset time to address the Year 2000 (Y2K) problem, applicable to records with year date data in "at least one of two-digit, three-digit, or four-digit" representations, was held anticipated by a system that offsets year dates in only two-digit formats). See also MPEP § 2131.02. "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). Note that, in some circumstances, it is permissible to use multiple references in a 35 U.S.C. 102 rejection.

See MPEP § 2131.01.

Rather than complying with the above-noted requirements, the Examiner has instead chosen to ignore claim features and/or mischaracterize the claim features. The Examiner however must, consistent with MPEP 2131, identify each and every element as set forth in the claim is found, either expressly or inherently described. This has clearly not been done in this case.

Furthermore, to the extent that the Examiner is basing the instant rejection on an argument of inherency consistent with MPEP 2112, Appellant notes that MPEP 2112 specifically states, in part:

"In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original) (Applicant's invention was directed to a biaxially oriented, flexible dilation catheter balloon (a tube which expands upon inflation) used, for example, in clearing the blood vessels of heart patients). The examiner applied a U.S. patent to Schjeldahl which disclosed injection molding a tubular preform and then injecting air into the preform to expand it against a mold (blow molding). The reference did not directly state that the end product balloon was biaxially oriented. It did disclose that the balloon was "formed from a thin flexible inelastic, high tensile strength, biaxially oriented synthetic plastic material." *Id.* at 1462 (emphasis in original). The examiner argued that Schjeldahl's balloon was inherently biaxially oriented. The Board reversed on the basis that the examiner did not provide objective evidence or cogent technical reasoning to support the conclusion of inherency.).

The Examiner has neither stated that the rejection is based on inherency, nor provided any basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.

Because the above-noted document fails to disclose, or even suggest, at least the above-

noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least independent claim 1.

REJECTION OF INDEPENDENT CLAIM 16 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 16 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited first and second registers and the recited combinational logic. Appellant respectfully disagrees and traverses this rejection.

As noted above, Appellant acknowledges that GREENE discloses an arrangement which utilizes an encryption circuit 102, an input buffer 104 and an output buffer 108 (see col. 5, lines 4-12). Appellant also acknowledges that GREENE discloses that the encryption circuit 102 utilizes “data encryption algorithms such as DES and Triple DES, or any of various secure hash algorithms” (see col. 6, lines 58-62). However, GREENE simply does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle.

The Examiner explains that the disclosed encryption circuit 102 of GREENE is same as the recited combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle. Appellant respectfully disagree. Again, an encryption circuit is not the *per se* same as combinational logic performing computation iterations of the crypto-function on data stored in

the first register and outputting data to the second register in a single hardware cycle. As explained on page 2, lines 2-9 of the instant application, conventional processing of crypto-functions require many clock and hardware cycles. As such processing typically occurs in an encryption circuit, the Examiner's apparent or implicit belief that all encryption circuits perform computation iterations of the crypto-function in a single hardware cycle lacks any support in the prior art.

Furthermore, while the Examiner has specifically pointed to col. 4, line 58 to col. 5, line 13 of GREENE (see page 2 of the Final Office Action) as disclosing the recited computation, the Examiner has failed to fully appreciate the fact that the noted language is entirely silent with regard to the terms "computational logic" and "crypto-function" and merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input buffer/working store 104, an output buffer 108, and a scheduler 106. An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L , where $L=nT$. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

There is simply no such disclosure in the above-noted language of GREENE and the Examiner has not demonstrated otherwise.

The Examiner also points to col. 5, lines 6-12 of GREENE as disclosing that the crypto-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read. This is incorrect. The noted language merely states the following:

An encryption circuit 102 can include a number of cipher stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L , where $L=nT$. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

The above-noted language simply does not disclose that the crypto-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read, and the Examiner has not demonstrated otherwise.

Appellant again submits that it is apparent from a fair reading the instant Final Office Action that the Examiner does not fully understand the requirements for a proper anticipation rejection. Appellant again directs the Examiner's attention to MPEP 2131 which was discussed above. Rather than complying with the above-noted requirements, the Examiner has instead chosen to ignore claim features and/or mischaracterize the claim features. The Examiner however must, consistent with MPEP 2131, identify each and every element as set forth in the claim is found, either expressly or inherently described. This has clearly not been done in this case.

Furthermore, to the extent that the Examiner is basing the instant rejection on an argument of inherency consistent with MPEP 2112, Appellant again refers the Examiner to

MPEP 2112 which was discussed above. At the very least, it is notable that the Examiner has neither stated that the rejection is based on inherency, nor provided any basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least independent claim 16.

REJECTION OF INDEPENDENT CLAIM 19 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 19 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited first and second registers and the recited combinational logic. Appellant respectfully disagrees and traverses this rejection.

As noted above, Appellant acknowledges that GREENE discloses an arrangement which utilizes an encryption circuit 102, an input buffer 104 and an output buffer 108 (see col. 5, lines 4-12). Appellant also acknowledges that GREENE discloses that the encryption circuit 102 utilizes “data encryption algorithms such as DES and Triple DES, or any of various secure hash algorithms” (see col. 6, lines 58-62). However, GREENE simply does not disclose, or even suggest, combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle.

The Examiner explains that the disclosed encryption circuit 102 of GREENE is same as the recited combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle.

Appellant respectfully disagree. Again, an encryption circuit is not the *per se* same as combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to the second register in a single hardware cycle. As explained on page 2, lines 2-9 of the instant application, conventional processing of crypto-functions require many clock and hardware cycles. As such processing typically occurs in an encryption circuit, the Examiner's apparent or implicit belief that all encryption circuits perform computation iterations of the crypto-function in a single hardware cycle lacks any support in the prior art.

Furthermore, while the Examiner has specifically pointed to col. 4, line 58 to col. 5, line 13 of GREENE as disclosing the recited computation, the Examiner has failed to fully appreciate the fact that the noted language is entirely silent with regard to the terms "computational logic" and "crypto-function" and merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

Referring now to FIG. 1, a block diagram is set forth illustrating a first embodiment. The first embodiment is designated by the general reference character 100, and is shown to include an encryption circuit 102, an input buffer/working store 104, an output buffer 108, and a scheduler 106. An encryption circuit 102 can include a number of cipher

P27325.A12

stages that enable pipelined operation. The encryption circuit 102 can process a given input data block with a latency L , where $L=nT$. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

There is simply no such disclosure in the above-noted language of GREENE and the Examiner has not demonstrated otherwise.

The Examiner also points to col. 5, lines 8-12 of GREENE as disclosing that the single hardware cycle comprises several clock cycles. This is incorrect. The noted language merely states the following:

The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

The above-noted language simply does not disclose that the single hardware cycle comprises several clock cycles, and the Examiner has not demonstrated otherwise.

Appellant again submits that it is apparent from a fair reading of the instant Final Office Action that the Examiner does not fully understand the requirements for a proper anticipation rejection. Appellant again directs the Examiner's attention to MPEP 2131 which was discussed above. Rather than complying with the above-noted requirements, the Examiner has instead chosen to ignore claim features and/or mischaracterize the claim features. The Examiner however must, consistent with MPEP 2131, identify each and every element as set forth in the claim is found, either expressly or inherently described. This has clearly not been done in this case.

Furthermore, to the extent that the Examiner is basing the instant rejection on an argument of inherency consistent with MPEP 2112, Appellant again refers the Examiner to

MPEP 2112 which was discussed above. At the very least, it is notable that the Examiner has neither stated that the rejection is based on inherency, nor provided any basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least independent claim 19.

REJECTION OF DEPENDENT CLAIM 2 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 2 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited block cipher algorithm of claim 2 in combination with the features of independent claim 1. Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms at col. 6, lines 58-67, GREENE does not disclose that such algorithms can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm of claim 2 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 2.

REJECTION OF DEPENDENT CLAIM 3 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 3 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited DES algorithm of claim 3 in combination with the features of claims 1 and 2. Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms such as DES at col. 6, lines 58-67, GREENE does not specifically disclose that a DES algorithm can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm of claim 3 and the features of claims 1 and 2 are simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 3.

REJECTION OF DEPENDENT CLAIM 4 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 4 under 35 U.S.C. § 102(e) as being anticipated by US Patent No.

6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited CHAIN algorithm of claim 4 in combination with the features of claims 1 and 2. Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms at col. 6, lines 58-67, GREENE does not specifically disclose that a CHAIN algorithm can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm of claim 4 and the features of claims 1 and 2 are simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 4.

REJECTION OF DEPENDENT CLAIM 5 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 5 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited algorithm operation. Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms at col. 6, lines 58-67, GREENE does not specifically disclose the recited algorithm operation can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm operation of claim 5 and the features of claims 1 and 2 are simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

For example, the Examiner is not correct that col. 7, lines 7-21 and col. 7, line 62 to col. 8, line 4 discloses that the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times. The noted language merely discloses the following:

In FIG. 4A, data blocks from different contexts are given a particular letter designation and number designation. The letter designation indicates a context of origin, the number designation indicates how many blocks have previously been processed for the context in question. Thus, a first context can provide data block A1, followed by data block A2, followed by data block A3, etc. Further, if it is assumed that CBC is employed, the encrypted form of data block A1 (designated as E[A1]) is an input that is used together with data block A2 to encrypt data block A2.

In general, each context will have its own encryption/decryption key (or, in the case of Triple-DES and similar algorithms, set of encryption/decryption keys). The keys for all active contexts are stored and retrieved at appropriate times as seen below.

A scheduler 106 can be programmed to provide appropriate priority to ensure feedback-type encryption operations. In particular, the active contexts can be stored, and on consecutive cycles, priority can be shifted to give the desired context priority. As shown in FIG. 4A, at time t14, priority can be shifted to give data block E1 priority. Further, one skilled in the art would recognize that the feedback loop in an encryption circuit would be disabled on this cycle to prevent the E_{KB} [B3] value from being combined with the E1 value.

Because the above-noted document fails to disclose, or even suggest, at least the above-

noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 5.

REJECTION OF DEPENDENT CLAIM 6 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 6 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited algorithm operation. Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms at col. 6, lines 58-67, GREENE does not specifically disclose the recited algorithm operation can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm operation of claim 6 and the features of claims 1 and 5 are simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

The Examiner is also not correct that col. 7, lines 7-21 and col. 8, lines 6-32 discloses that the combinational logic performs mixing, permutation and key-dependent substitution in each round. The noted language merely discloses the following:

In FIG. 4A, data blocks from different contexts are given a particular letter designation and number designation. The letter designation indicates a context of origin, the number designation indicates how many blocks have previously been processed for the context in question. Thus, a first context can provide data block A1, followed by data block A2, followed by data block A3, etc. Further, if it is assumed that CBC is employed, the encrypted form of data block A1 (designated as E[A1]) is an input that is used together

with data block A2 to encrypt data block A2.

In general, each context will have its own encryption/decryption key (or, in the case of Triple-DES and similar algorithms, set of encryption/decryption keys). The keys for all active contexts are stored and retrieved at appropriate times as seen below.

In an alternate embodiment, a system may include as many contexts as there are pipeline stages. Each context can be accessed sequentially. In the event a context does not include a data block, a read from the input buffer and write to the output buffer can be suppressed.

In this way, an encryption system can provide an encrypted data block in each system cycle for feedback-type encryption. This is in contrast to a conventional approach that may supply a first data block of a sequence to an encryption circuit and then supply the second block a predetermined time later, limited by the latency of the encryption process on the first data block. Thus, the present invention can process a data block on each system cycle (provided sufficient contexts are active) even when the encryption function includes a feedback loop.

While the above description has described the particularly useful application of the invention to encryption, the described embodiments could also be utilized in other computations, such as modular exponentiation, as but one example. As one very particular example, if the method described in the background above is employed to compute $y=(A^e) \bmod n$, a modular multiply computation circuit (in place of the encryption circuit 102) could provide the $yy=(yy*aa) \bmod n$ operation and/or the $aa=(aa*aa) \bmod n$ operation. Of course, the scheduler operation could be adjusted to ensure that the $yy=(yy*aa) \bmod n$ operation is performed only for iterations corresponding to an "e" bit value equal to one.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 6.

REJECTION OF DEPENDENT CLAIM 7 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 7 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be

reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited algorithm operation. Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms at col. 6, lines 58-67, GREENE does not specifically disclose the recited algorithm operation can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm operation of claim 7 and the features of claims 1 and 5 are simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

The Examiner is also not correct that col. 7, lines 51-67 discloses that the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation. The noted language merely discloses the following:

Once four values are read into an encryption pipeline, corresponding second data blocks must be read in a predetermined order to ensure proper feedback-type encryption. Because more data blocks are present in the sequences corresponding to contexts 400-1 to 400-4, data blocks A2, B2, C2 and D2 are input at times t5 to t8. At the same time, encrypted data values E_{KA} [A1,IVA], E_{KB} [B1,IVB], E_{KC} [C1,IVC] and E_{KD} [D1,IVD] are provided as output values and, internal to the encryption circuit, as feedback values for combination with data blocks A2, B2, C2 and D2, respectively.

A scheduler 106 can be programmed to provide appropriate priority to ensure feedback-type encryption operations. In particular, the active contexts can be stored, and on consecutive cycles, priority can be shifted to give the desired context priority. As shown in FIG. 4A, at time t14, priority can be shifted to give data block E1 priority.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 7.

REJECTION OF DEPENDENT CLAIM 8 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 8 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited algorithm operation. Appellant respectfully disagrees that GREENE discloses that the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process, and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data encryption algorithms at col. 6, lines 58-67, GREENE does not specifically disclose the recited algorithm operation can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm operation of claim 8 and the features of claims 1, 2, 5 and 7 are simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 8.

REJECTION OF DEPENDENT CLAIM 9 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 9 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, one hardware cycle of approximately ten clock cycles.

Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 5, lines 7-12 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. The noted language of GREENE merely states the following:

The encryption circuit 102 can process a given input data block with a latency L, where $L=nT$. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

The combination of the recited clock cycles of claim 9 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 9.

REJECTION OF DEPENDENT CLAIM 10 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 10 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be

reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, not storing intermediate results in registers. Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 4, lines 58-67 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. Again, the noted language of GREENE merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

The combination of the recited features of claim 10 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 10.

REJECTION OF DEPENDENT CLAIM 11 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 11 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim

including, among other features, the recited iterated round function in one hardware cycle.

Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 5, lines 7-12 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. Again, the noted language of GREENE merely states the following:

The encryption circuit 102 can process a given input data block with a latency L, where $L=nT$. The value n can be the number of cipher stages, and the value T is the clock period of the system, which will be no smaller than the delay introduced by the slowest cipher stage.

The combination of the recited features of claim 11 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 11.

REJECTION OF DEPENDENT CLAIM 12 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 12 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the recited DES algorithm in combination with claim 1.

Appellant respectfully disagrees and traverses this rejection.

While it is apparent that GREENE discloses using various types of known data

encryption algorithms such as DES at col. 6, lines 58-67, GREENE does not specifically disclose that a DES algorithm can be used with, among other things, the recited combinational logic of claim 1 (for the reasons noted above). The combination of the recited algorithm of claim 12 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 12.

REJECTION OF DEPENDENT CLAIM 13 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 13 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, that the combinational logic utilizes logic functions whose outputs depend solely on their inputs. Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 5, lines 12-23 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. Again, the noted language of GREENE merely states the following:

The input buffer/working store 104 can include various storage circuits that store data blocks from multiple data streams. Each data stream can include one data block, or a sequence of data blocks having a particular order. Each such data block and/or sequence of data blocks will be referred to herein as a "context." As just one example, each context

can represent data from a particular network packet. An input buffer/working store 104 can be implemented in a variety of forms. As but two of the many possible examples, an input buffer can include first-in-first-out (FIFO) memory device(s) or random access memory (RAM) device(s).

The combination of the recited features of claim 13 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 13.

REJECTION OF DEPENDENT CLAIM 14 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 14 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, that the combinational logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of enciphering or deciphering computations. Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 4, lines 29-67 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. The relevant portion of noted language of GREENE merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each

operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

The combination of the recited features of claim 14 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 14.

REJECTION OF DEPENDENT CLAIM 15 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 15 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, the crypto-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read. Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 4, lines 58-67 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. Again, the noted language of GREENE merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

The combination of the recited features of claim 15 and the features of claim 1 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 15.

REJECTION OF DEPENDENT CLAIM 17 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 17 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, one hardware cycle of approximately ten clock cycles.

Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 4, lines 58-67 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. The noted language of GREENE merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

The combination of the recited clock cycles of claim 17 and the features of claim 16 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 17.

REJECTION OF DEPENDENT CLAIM 18 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 18 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, that the hardware implementation of the crypto-function computes an iterated round function in just one clock cycle. Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 4, lines 58-67 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. Again, the noted language of GREENE merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

Such language is not the same as computing an iterated round function in just one clock cycle. As such, the combination of the recited features of claim 18 and the features of claim 16 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated

otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 18.

REJECTION OF DEPENDENT CLAIM 20 UNDER 35 U.S.C. § 102 IS IN ERROR

The rejection of claim 20 under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,870,929 to GREENE is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

The Examiner asserted that GREENE discloses all of the features recited in this claim including, among other features, not storing intermediate results in registers. Appellant respectfully disagrees and traverses this rejection.

While the Examiner has identified col. 4, lines 58-67 of GREENE as disclosing this feature, it is clear that the Examiner is incorrect. Again, the noted language of GREENE merely states the following:

Various embodiments of the present invention will now be described in conjunction with a number of diagrams. The various embodiments include an encryption system that can provide higher throughput than other conventional approaches. In particular embodiments, multiple data blocks can be pipelined across one or more encryption circuits. Such an arrangement can allow a new encrypted block to be generated on each operational cycle, where a cycle can be as small as one clocked cipher stage within an encryption circuit.

The combination of the recited features of claim 20 and the features of claim 19 is simply not disclosed or suggested in GREENE, and the Examiner has not demonstrated otherwise.

Because the above-noted document fails to disclose, or even suggest, at least the above-

noted features of the instant invention, Appellant submits that no proper reading of GREENE renders anticipated the combination of features recited in at least dependent claim 20.

(VIII) CONCLUSION

Each of claims 1-20 are patentable under 35 U.S.C. § 102(e). Specifically, the applied art of record fails to disclose or suggest the unique combination of features recited in Appellants' claims 1-20. Accordingly, Appellant respectfully requests that the Board reverse the decision of the Examiner to reject claims 1-20 under 35 U.S.C. §102(e), and remand the application to the Examiner for withdrawal of the above-noted rejections.

Please charge any deficiencies in fees and credit any overpayment of fees to Deposit Account No. 50-0563.

Respectfully submitted,
J. L. CALVIGNAC et al.



Andrew M. Calderon
Reg. No. 38,093

December 20, 2006
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
703-716-1191

Attachments:

Claims Appendix
Evidence Appendix
Related Proceedings Appendix

CLAIMS ON APPEAL

1. A hardware implementation of a crypto-function comprising:
a first register storing data to be encrypted or decrypted;
a second register for receiving data which has been encrypted or decrypted; and
combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

2. The hardware implementation of a crypto-function recited in claim 1, wherein the crypto-function is a block cipher algorithm.

3. The hardware implementation of a crypto-function recited in claim 2, wherein the crypto-function is the Data Encryption Standard (DES) algorithm.

4. The hardware implementation of a crypto-function recited in claim 2, wherein the crypto-function is the CHAIN algorithm.

5. The hardware implementation of a crypto-function recited in claim 2, wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times.

6. The hardware implementation of a crypto-function recited in claim 5, wherein the combinational logic performs mixing, permutation and key-dependent substitution in each round.

7. The hardware implementation of a crypto-function recited in claim 5, wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation.

8. The hardware implementation of a crypto-function recited in claim 7, wherein the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process.
9. The hardware implementation of a crypto-function recited in claim 1, wherein the one hardware cycle is approximately ten clock cycles.
10. The hardware implementation of a crypto-function recited in claim 1, wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers.
11. The hardware implementation of a crypto-function recited in claim 1, wherein the hardware implementation of the crypto-function computes an iterated round function in one clock cycle.
12. The hardware implementation of a crypto-function recited in claim 1, wherein the combinational logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combinational logic.
13. The hardware implementation of a crypto-function recited in claim 1, wherein the combinational logic utilizes logic functions whose outputs depend solely on their inputs.
14. The hardware implementation of a crypto-function recited in claim 1, wherein the combinational logic utilizes logic circuits without memory, whereby no registers are used to store intermediate results or iterations of enciphering or deciphering computations.
15. The hardware implementation of a crypto-function recited in claim 1, wherein the crypto-function is implemented in the combinational logic without intermediate registers that
(P27325 00104623.DOC)

require loading and settling time before contents of the intermediate registers can be read.

16. A hardware implementation of a crypto-function comprising:
a first register that stores data to be encrypted or decrypted;
a second register that receives data which has been encrypted or decrypted; and
combinational logic that performs computation iterations of the crypto-function on data
stored in the first register and outputting data to said second register in a single hardware cycle,
wherein the crypto-function is implemented in the combinational logic without
intermediate registers that require loading and settling time before contents of the intermediate
registers can be read.

17. The hardware implementation of a crypto-function recited in claim 16, wherein the
single hardware cycle is approximately ten clock cycles.

18. The hardware implementation of a crypto-function recited in claim 16, wherein the
hardware implementation of the crypto-function computes an iterated round function in just one
clock cycle.

19. A hardware implementation of a crypto-function comprising:
a first register that stores data to be encrypted or decrypted;
a second register that receives data which has been encrypted or decrypted; and
combinational logic that performs computation iterations of the crypto-function on data
stored in the first register and outputting data to said second register in a single hardware cycle,
wherein the single hardware cycle comprises several clock cycles.

20. The hardware implementation of a crypto-function recited in claim 19, wherein the
crypto-function is implemented in the combinational logic without intermediate registers that
require loading and settling time before contents of the intermediate registers can be read.

EVIDENCE APPENDIX

This section lists evidence submitted pursuant to 35 U.S.C. §§1.130, 1.131, or 1.132, or any other evidence entered by the Examiner and relied upon by Appellant in this appeal, and provides for each piece of evidence a brief statement setting forth where in the record that evidence was entered by the Examiner. Copies of each piece of evidence are provided as required by 35 U.S.C. §41.37(c)(ix).

NO.	EVIDENCE	BRIEF STATEMENT SETTING FORTH WHERE IN THE RECORD THE EVIDENCE WAS ENTERED BY THE EXAMINER
1	N/A	N/A

RELATED PROCEEDINGS APPENDIX

Pursuant to 35 U.S.C. §41.37(c)(x), copies of the following decisions rendered by a court of the Board in any proceeding identified above under 35 U.S.C. §41.37(c)(1)(ii) are enclosed herewith.

NO.	TYPE OF PROCEEDING	REFERENCE NO.	DATE
1	N/A	N/A	N/A